［セキュリティ人材育成の現状と実践］

①セキュリティ人材育成の現状と今後の展望―持続的なセキュリティ人材の供給に向けて―

衛藤将史 | 国立研究開発法人情報通信研究機構
神薗雅紀 | デロイトトーマツ サイバー合同会社

セキュリティ人材の不足

IT インフラの普及とともにサイバー攻撃は多様化，高度化しており，近年では政府機関や，電気，ガス，水道等の重要インフラも攻撃の対象になるなど，国民生活の脅威となっている．長年にわたりセキュリティ対策技術の整備や研究開発が世界的に進められているが，とりわけ日本においては第 32 回オリンピック競技大会（2020／東京）および東京 2020 パラリンピック競技大会に向けたセキュリティ対策も重要な課題となっている．このようなセキュリティ対策の必要性の高まりを受けて，官民挙げての施策が進む中で顕在化してきたのが，慢性的なセキュリティ人材の不足である．

ここでいう「セキュリティ人材」とは，専門企業においてセキュリティ技術の研究開発等に取り組む人材や，システムインテグレータ（SI），ユーザ企業等においてセキュリティ対策の構築・運用を担う人材を指す．

そのため現在，国内外において，さまざまな形態のセキュリティ人材育成プログラムや標準化等，人材不足への対応が進められている．しかし，社会情勢がめまぐるしく変化する時代において，国内外で実施されているセキュリティ人材育成は，その内容，効率性，カバレッジといった観点で，人材需要にそぐわない可能性がある．

そこで本稿では，社会全体としてセキュリティ人材育成を戦略的に進めるため，主に高等教育から社会人教育を対象として，国内外のセキュリティ人材育成に関する状況を俯瞰する．特に国内の複数のセキュリティ人材育成プログラムの関係者とユーザ企業への聞き取り調査を通じて，人材育成における課題を明らかにし，その結果をふまえ，今後の社会において必要な取組みについて提言する．

国内外における状況

諸外国の状況

日本と同様に，諸外国においてもセキュリティ人材の不足が，長年の社会的な課題となっている．米国においては人材育成の必要性が早くから指摘されていたことから，主に民間での対応が他国と比較して進んでいるのに加え，政府主導の取組みも積極的に行われている．米国では民間企業によるセキュリティ企業や業界団体が発行する技能認定が普及しており，企業における職員募集の際に，これらの資格を雇用条件とする場合が多い．特に（ISC）[2☆1] による CISSP[☆2] や，情報システム監査・情報セキュリティの専門家団体 ISACA[☆3] が提供する CISA，IT

☆1 The International Information System Security Certification Consortium, https://www.isc2.org/
☆2 Certified Information Systems Security Professional, https://www.isc2.org/Certifications/CISSP
☆3 Information Systems Audit and Control Association, https://www.isaca.org/pages/default.aspx

関連の資格認定を行う業界団体 CompTIA[☆4] による Security+[☆5] 等の資格が，広く認知・取得されている．また，政府機関による取組みとして，米国商務省 国立標準技術機関（NIST）[☆6] が中心となって推進する The National Initiative for Cybersecurity Education（NICE）では，人材育成の在り方に関する議論や，産学官の連携強化，セキュリティ人材のキャリアパスの整備などを進めている[1]．NICE フレームワーク（NIST SP800-181）[☆7] は，セキュリティ関連業務における役割や専門分野，必要とされる知識や能力等をよく体系化しており，米国外の組織においても多く参照されている．

欧州においては，European Network and Information Security Agency（ENISA）が欧州連合（EU）としてのサイバーセキュリティ戦略を策定・牽引しており，その中で人材育成にも取り組んでいる[2]．CyberEurope[☆8] は，ENISA が主催する欧州最大規模の非軍事サイバー演習であり，ENISA が提供するサイバー演習プラットフォーム（Cyber Exercise Platform）を活用し，電力，航空産業等，主に重要インフラを対象としたサイバー攻撃への備えを進めている．また，域内の各国も独自にセキュリティ人材育成施策を推進しており，セキュリティ教育の体系化が比較的進むイギリスとエストニアでは，国家サイバーセキュリティセンター（NCSC）や防衛省が中心となって，各年代に見合ったセキュリティ教育プログラムや若手人材の早期発掘プログラム等を推進している．イギリスの NCSC 等が実施する CyberFirst[☆9] は，11 歳から 17 歳の若年層へのサイバーセキュリティ技術の習得機会の提供と，将来のセキュリティ人材の発掘を目的とし，年齢層ごとに段階的な教育プログラムを用意している．CyberSpike[☆10] は，エストニアの防衛省等が実施する 14 歳から 25 歳までの若年層向けのセキュリティ人材発掘・育成プログラムであり，サイバー防御演習や攻撃技術に関する座学講座，サイバー防御演習の競技会等を行っている．

国内の状況

公的な人材育成の概況

日本におけるセキュリティ人材の不足は社会的な課題となっており，産学官それぞれが対策に取り組んでいる．政府の取組みとしては，内閣サイバーセキュリティセンター（NISC）[☆11] がサイバーセキュリティ戦略に基づき，各省庁における施策への指導を行っている[3]．

主に社会人を対象とする施策として，情報処理推進機構（IPA）の産業サイバーセキュリティセンター（ICSCoE）[☆12] が推進する中核人材育成プログラムでは，セキュリティ対策の強化をテーマに，経営層と現場担当者を繋ぐ人材（中核人材）の育成に取り組んでいる．なお ICSCoE は，このほかにも国際トレーニング[☆13]，業界別サイバーレジリエンス強化演習[☆14]，戦略マネジメント系セミナー[☆15]，制御システム向けサイバーセキュリティ演習[☆16] 等の多様なプログラムを展開している．また IPA では，情報処理安全確保支援士（RISS）[☆17]，セキュリティマネジメント試験等，より実践的な資格認定事業を推進している．

一方，若年層を対象とした人材育成施策とし

☆4 The Computing Technology Industry Association, https://www.comptia.jp/
☆5 https://www.comptia.jp/certif/core/comptia_security/
☆6 https://www.nist.gov/itl/applied-cybersecurity/nice
☆7 https://csrc.nist.gov/publications/detail/sp/800-181/final
☆8 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
☆9 https://www.cyberfirst.ncsc.gov.uk/
☆10 https://sites.google.com/view/kyberolympia/eng
☆11 https://www.nisc.go.jp/
☆12 https://www.ipa.go.jp/icscoe/
☆13 https://www.ipa.go.jp/icscoe/program/short/all_industries/index.html
☆14 https://www.ipa.go.jp/icscoe/program/short/specific_industries/index.html
☆15 https://www.ipa.go.jp/icscoe/program/middle/strategic_management/index.html
☆16 https://www.ipa.go.jp/icscoe/program/middle/strategic_management/index.html
☆17 https://www.ipa.go.jp/siensi/

ては，情報通信研究機構（NICT）において若手セキュリティイノベータの育成を目的としたSecHack365[☆18]と呼ばれる，1年間の演習プログラムを実施しているほか，国立高等専門学校機構では，全国の高専が連携し，セキュリティ演習やコンテストを中心とした情報セキュリティ人材育成プログラム（K-SEC）[☆19]を推進している．

NICTが実施する実践的サイバー防御演習CYDERは，公的機関や民間組織のセキュリティレベルの底上げのため，一連のインシデント対応を実機演習の形式で学ぶ，1日間の教育プログラムである．

人材育成プログラムの具体例

ここでは官民で行われている取組みから，いくつか例を挙げて，事業の具体的な内容を紹介する．

IPAは前述のICSCoEのほかに，セキュリティ・キャンプ協議会とともにセキュリティ・キャンプ[☆20]事業を推進している．セキュリティ・キャンプは，高度な技術を持つ各分野の専門家が，実習を交えながら学生にセキュリティ関連技術を指導するプログラムである．毎年8月に東京で行われるセキュリティ・キャンプの全国大会では，22歳以下の学生・生徒を対象に5日間での集中的な講座が展開される．

日本ネットワークセキュリティ協会（JNSA）が主催するSECCON[☆21]（セクコン）では，実践的なセキュリティ人材の発掘・育成，技術の実践の場の提供を目的として，情報セキュリティをテーマにCapture The Flag（CTF）[☆22]を中心とした多様な競技会が開催されている．東京において2日間で開催される決勝大会には1,000名を超える来場者（2018年実績）が訪れる．

SecCap[☆23]は，文部科学省が推進する教育事業enPiTのうち，セキュリティ分野を担うプログラムである．複数の大学が連携し，セキュリティ理論から応用まで網羅的に，座学と実習を交えた教育を通年で行う．SecCapの前身は，関西圏の4つの情報系大学院を中心として実施されたIT-Keys[☆24]と呼ばれる教育プログラムであり，その当時から，組織横断的な教育と受講生同士の交流に力を入れてきた．

Hardening競技会[☆25]は，WASForum Hardening Project実行委員会が主催する，ECサイトの防御に特化した競技形式のセキュリティイベントであり，Webサイトの安全性を追求する技術の啓発と人材の育成を目的としている．ほかのCTFと大きく異なるのは，組織ネットワークの堅牢化だけでなく，企業利益の最大化をもテーマとした，総合的なセキュリティ競技会という点である．参加者は，イベント運営者が用意した模擬ECサイトを攻撃から守り，そのECサイトの収益を最大化することを目指す．

本会が主催するマルウェア対策研究人材育成ワークショップ（MWS）[☆26]は，セキュリティ対策技術の研究者・開発者の育成を目的として例年開催される研究会である．国内の研究機関等から提供されたサイバー攻撃関連データセットを主催者が参加希望者に事前に共有し，ワークショップ当日にそのデータセットを利用した研究成果が発表される．セキュリティの研究には適切なデータセットが不可欠だが，これを主催者が一元的に提供することで，研究者が成果を相互に比較することが可能となり，結果として研究の質が向上した．

人材育成における課題

前章で紹介したとおり，現在，人材育成に関する取組みが盛んに行われてはいるが，必要十分な人材

☆18 https://sechack365.nict.go.jp
☆19 https://csinfo2018.kochi-ct.ac.jp/
☆20 https://www.ipa.go.jp/jinzai/camp/
☆21 https://www.seccon.jp/
☆22 パケット分析，プロトコル解析，システム管理，プログラミング，暗号解読等のセキュリティ技術の競技会．
☆23 https://www.seccap.jp/
☆24 http://it-keys.naist.jp/
☆25 https://wasforum.jp/hardening-project/
☆26 https://www.iwsec.org/mws/

を供給するには，まだ多くの課題がある．それらの中でも，とりわけ筆者が重要と考える次の 2 点について述べる．

1. セキュリティ人材の需要（雇用）と供給（教育）が適切に対応しているか
2. 人材モデルやスキルマップが活用されているか

セキュリティ人材の需要と供給の対応状況

輩出される人材が社会で活躍するためには，身につけた知識や技術が，就職先企業でのキャリアに結びついていることが重要である．そこで筆者らは国内の人材育成プログラムの中で，より認知度が高いと思われる 6 事業の関係者に対して，育成に注力している人材モデルや技術領域等に関する聞き取り調査を行った．

また，輩出される人材の主な就職先となる国内のユーザ企業のうち，製造業やサービス業等を含む 29 社の事業部門の担当者に対しても同様に，必要とする人材モデルや技術領域について聞き取り調査をした．その上で，これらの調査結果を重ね合わせて，人材育成にかかわる需要と供給の対応状況について考察する．

調査項目の 1 点目として，人材モデルを「ジェネラリスト／スペシャリスト」「経営者側／現場側」という 2 軸で定義し，4 つの象限から育成に注力する人材，必要とする人材を尋ねた（2 つまで選択可）．図 -1 に示す各グラフは，各事業・企業が選択した人材モデルの合計を示している．その結果，今回の調査対象となった人材育成プログラムにおいては，現場寄りで，ややジェネラリスト寄りの人材の育成に取り組む傾向が見られた．一方ユーザ企業側は，よりジェネラリストを指向する傾向があり，また，現場よりも経営側に立てる人材を望んでいることが分かった．

2 点目として，技術領域に関する指向について尋ねた．ネットワークセキュリティ，ストラテジ／ガバナンス，Web セキュリティ，OS セキュリティ，データベースセキュリティ，フォレンジクス，バイナリ解析の 7 つの領域について，人材育成プログラムが注力している技術とユーザ企業が技術者に求める技術とを尋ねた．各項目について注力の度合いを 1 ～ 4 点で示したものを対象者から集め，項目ごとに平均化している．

図 -2 はユーザ企業が求める技術（赤線）を平均値の大きいものから順に並べたものである．この図によると，ユーザ企業がネットワークセキュリティ，ストラテジ／ガバナンス，Web セキュリティ等の

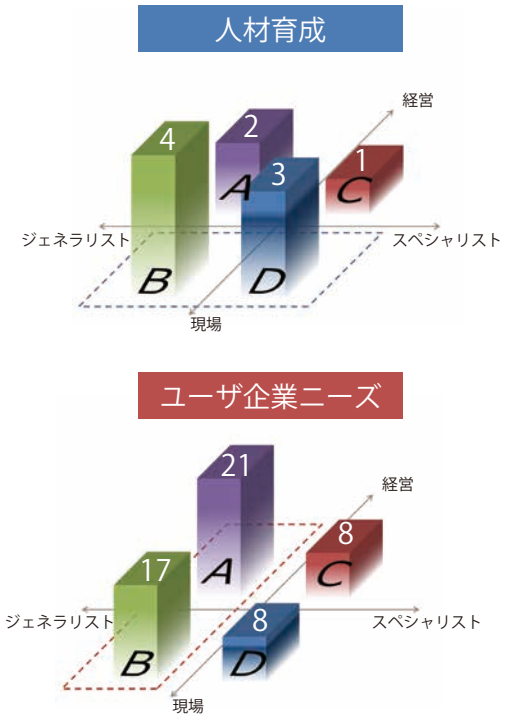

図 -1　人材育成とユーザ企業ニーズの傾向

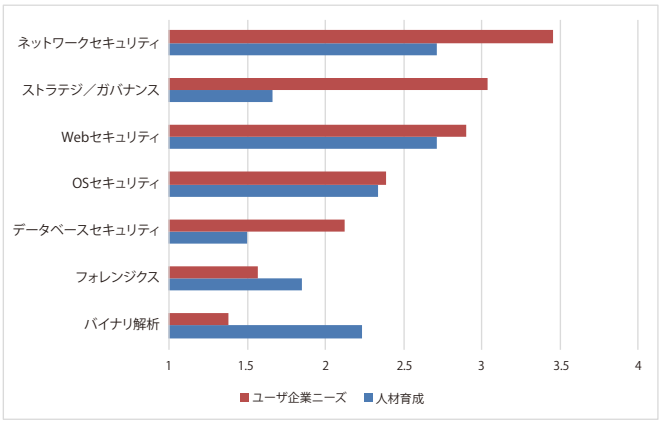

図 -2　ユーザ企業ニーズと人材育成プログラムの傾向

知識を持つ技術者を求めている一方で，人材育成プログラム（青線）では，それらに加えて，OS セキュリティやフォレンジクス☆27，バイナリ解析等の幅広い指導に力を入れていることが分かる．

両者の差が顕著なのは，セキュリティに関する戦略や，中長期的な計画の立案を主な内容とするストラテジ／ガバナンスの項目である．ユーザ企業がストラテジ／ガバナンス関連の知識を有する技術者を求めているのに対して，今回の調査対象の人材育成プログラムにおいては，この領域の教育はそれほど活発ではない．実際には，これらの技術領域に関する教育プログラムが提供されてはいるが，主な受講者である若手技術者層は，より現場寄りの技術を指向する傾向があるため，参加者が多く集まりにくいという実態がある．

また，人材育成プログラムでは，サイバー攻撃の痕跡を探し出すフォレンジクスや，マルウェア等のプログラムの機能を明らかにするバイナリ解析にも比較的に力を入れている反面，ユーザ企業においては，この技術を有する人材のニーズはそれほど大きくない点も特徴的である．その理由は，これらの技術はより専門性が高く，習得に時間がかかることから，ユーザ企業ではセキュリティの専門企業に外部委託するのが一般的なためである．

このようなミスマッチは，人材育成と企業における採用の現場にも影響を与えている．

その具体例として，人材育成関係者への聞き取りにおいて，「学生にとっての育成プログラムでの経験が，就職に直結しないケースがある」といった意見があった．すなわち，人材育成プログラムにおいて高いレベルのセキュリティ技術を身につけたが，就職先として選択したユーザ企業ではその技術を活かすことができず，短期間で転職をしてしまうケースが見られたとのことである．

このようなミスマッチの原因の１つとして，育成プログラムを提供する側と参加する側の意識の差が挙げられる．現状において，若手のセキュリティ人材は図 -1 における現場寄りの技術の習得指向が強い．結果として，育成プログラムの提供者がユーザ企業のニーズに合わせて経営寄りのメニューを用意しても，十分な参加者を確保しづらい傾向がある．そのため，経営寄りのキャリアの魅力や技術の重要性を若手のセキュリティ人材層に訴えていく工夫が必要である．

人材モデルとスキルマップの活用

前章で述べた需要と供給のミスマッチを少しでも減らすためには，セキュリティ技術の習得を志す者のみならず，育成プログラム提供者，採用担当者等，セキュリティ人材にかかわるすべての人が，同じスキルマップを用いることが重要である．

その理由は，育成プログラム提供者が教育コンテンツを製作する際の基礎として，またセキュリティ技術の習得を目指す者が学習計画やキャリアを検討する際のガイドラインとして，さらに企業において適正な人材の確保や組織内のキャリアパスの検討材料として，共通した指標を使用すれば，学習の効率が高まる上に，キャリアに関する認識の不一致を防ぐこともできるからである．

その点，日本ではすでに教育機関から産業界まで幅広く利用可能な複数のスキルマップが発行されている．2017 年度に公開された IPA の ITSS+☆28 は，セキュリティ領域における具体的な専門分野や業務活動，必要なスキルを体系化した指標である．また，日本ネットワークセキュリティ協会（JNSA）が発行する SecBoK☆29 は，前述の NIST における NICE フレームワーク（NIST SP800-181）を基盤としたスキルマップであり，多くの教育機関や企業において利用されている．なお，筆者が本務において担当している CYDER 事業でも，SecBoK に基づいた学習コンテンツを作成している．さらに，情報セキュリティ教育事業者連絡会（ISEPA）では，

☆27 電子機器の中からサイバー攻撃の証拠や手がかりを探し出す取組み．

☆28 https://www.ipa.go.jp/jinzai/itss/itssplus.html

☆29 https://www.jnsa.org/result/2018/skillmap/

JTAGと呼ばれるプロジェクトにおいて，セキュリティ人材のスキル可視化ガイドラインを公開している．JTAGはITSSやSecBoK等の既存のフレームワークを土台としており，JTAGの可視化ツールを用いると，個人が有する資格や業務経験等を入力することで，その個人のスキルをレーダーチャート等で表示することが可能となる[4]．

これらのスキルマップやガイドラインはすでに，人材育成の現場からユーザ企業まで広く利用されはじめているが，その認知度をより広めていくことが大切である．

持続的なセキュリティ人材の供給に向けて

筆者らが海外の人材育成関係者に対しても聞き取り調査を行ったところ，前節で述べたような人材育成にまつわる状況は，海外でも同様であることが分かった．たとえば欧州においても人材の需要に供給が追いついておらず，また教育内容が必ずしもニーズに合っていない部分もある．現時点では，欧州全体として人材を持続的に供給可能な体系的なシステムは構築されていない状況である．

このように世界的に共通する状況の背景には，教育の成果の短期的な見えにくさ，関係者の長期的なモチベーションの維持，インストラクタの訓練，そして予算の確保といった諸々の課題が横たわっている．これらを解消し，持続的なセキュリティ人材の供給体制を社会的に築くには，まずは先に述べた需要と供給のバランスとスキルマップの活用が不可欠である．

その上で，たとえば次のように対象者層ごとに適切な人材育成・流通のための施策を行うことが望ましい．

前期中等教育期

早期にセキュリティ意識を植え付けるための教育を行う

後期中等教育期

セキュリティに特化した学位やカリキュラムを整備する

一般社会人向け

事業規模・事業領域ごとに異なる教育プログラムと資格を提供する

全般向け

米国のNational Initiative for Cybersecurity Careers and Studies（NICCS）☆30のようなセキュリティに特化したキャリア支援サイトを政府主導で運営する

以上のような取組みに加えて，育成プログラムから輩出された人材が活躍できるような人事制度などを整備することで，セキュリティ人材のエコシステムを構築することも重要である．

持続的なセキュリティ人材の供給体制の実現には，これらの施策を産学官が連携して1つずつ着実に積み重ねていくことが，最も近道であると筆者は考える．

参考文献

1) NICE : National Initiative For Cybersecurity Education, https://www.nist.gov/itl/applied-cybersecurity/nice
2) ENISA : Cybersecurity Education Snapshot for Workforce Development in the EU (2015), https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/view
3) NISCサイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ：報告書，～「戦略マネジメント層」の育成・定着に向けて～（2018）．
4) JNSA情報セキュリティ教育事業者連絡会（ISEPA）：セキュリティ業務を担う人材のスキル可視化ガイドライン～プラス・セキュリティ人材の可視化に向けて～ β版（2019）．

(2019年6月3日受付)

衛藤将史　eto@nict.go.jp

2005年奈良先端科学技術大学院大学情報科学研究科博士後期課程修了．同年，情報通信研究機構に入所．以降，ネットワーク技術とサイバーセキュリティ技術の研究開発，国際標準化，人材育成に取り組む．

神薗雅紀　masaki.kamizono@tohmatsu.co.jp

2005年徳島大学大学院博士前期課程知能情報工学修了．2019年デロイトトーマツ サイバー合同会社 サイバーセキュリティ先端研究所所長に就任．サイバーセキュリティの研究開発，ソリューション開発，人材育成に取り組む．

☆30 https://niccs.us-cert.gov/training/search